

How Cloudflare works

Fundamentally, Cloudflare is a large network of servers that can improve the security, performance, and reliability of anything connected to the Internet.

Cloudflare does this by serving as a reverse proxy [↗](#) for your web traffic. All requests to and from your origin flow through Cloudflare and — as these requests pass through our network — we can apply various rules and optimizations to improve security, performance, and reliability.

Life of a request

Even though it feels pretty instantaneous, there's a lot happening when you type `www.example.com` into your browser.

A website's content does not technically live at a URL like `www.example.com`, but rather at an IP address like `192.0.2.1`. It's similar to how we say that Cloudflare's headquarters is 101 Townsend St., San Francisco, CA 94107, but really that address is just a placeholder for latitude and longitude coordinates (37.780259, -122.390519). URLs and street addresses are much easier for humans to remember.

The process of converting a human-readable URL (`www.example.com`) into a machine-friendly address (`192.0.2.1`) is known as a DNS lookup [↗](#).

Without Cloudflare

Without Cloudflare, DNS lookups for your application's URL return the IP address of your origin server [↗](#).

URL	Returned IP address
-----	---------------------

<code>example.com</code>	<code>192.0.2.1</code>
--------------------------	------------------------

When using Cloudflare with unproxied DNS records, DNS lookups for unproxied domains or subdomains also return your origin's IP address.

Another way of thinking about this concept is that visitors directly connect with your origin server.

Visitor <-[Connection]-> Origin Server

With Cloudflare

With Cloudflare — meaning your domain or subdomain is using proxied DNS records — DNS lookups for your application’s URL will resolve to Cloudflare Anycast IPs [↗](#) instead of their original DNS target.

URL	Returned IP address
example.com	104.16.77.250

This means that all requests intended for proxied hostnames will go to Cloudflare first and then be forwarded to your origin server.

Visitor <-[Connection 1]-> Cloudflare Edge <-[Connection 2]-> Origin Server

Benefits

When your traffic is proxied through Cloudflare before reaching your origin server, your application gets additional security, performance, and reliability benefits.

Security

Beyond hiding your origin’s IP address from potential attackers, Cloudflare also stops malicious traffic before it reaches your origin web server.

Cloudflare automatically mitigates security risks using our WAF and DDoS protection .


You can also set up additional protection with Firewall rules , Rate Limiting rules , IP access rules [↗](#), and other tools [↗](#).

Performance

For proxied traffic, Cloudflare also serves as a Content Delivery Network (CDN) [↗](#), caching static resources and otherwise optimizing asset delivery.

For additional details on performance, refer to our guides on [Optimizing Site Speed](#) and [Caching](#) .

Reliability

Cloudflare's globally distributed [Anycast network](#)  routes visitor requests to the nearest Cloudflare data center.

Combined together with our [CDN](#)  and [DDoS protection](#) , our network helps keep your application online.

[Edit on GitHub](#)  · Updated 4 hours ago